CLAIMS

We claim:

1. An improved method of encryption for the transmission of information comprising the steps of:

creating an encryption key;

limiting access to an encryption key;

registering an account owner; and

registering a communication device.

2. A method as recited in claim 1 wherein said access to the encryption key is limited to a Transmitting and a Receiving Device.

3. A method as recited in claim 1 wherein said registration of an account comprises:

the registration of a device owner with a Recipient Device; and

the registration of a Transmitting Device with a Recipient Device.

4. A method as recited in claim 3 wherein said registration of an account occurs in an automated manner without user intervention.

5. A method as recited in claim 1, further comprising the step of integrating the encryption key with the communication device hardware.

6. A method as recited in claim 1, further comprising the step of encrypting and decrypting information at speeds that do not impede communication rates.

7. An apparatus for encryption utilizing a combination of hardware and software comprising:

a Transmitting Device;

a Recipient Device;

a message package; and

means for executing algorithm for encryption, decryption and registration.

8. An apparatus as recited in claim 7 wherein said recipient device comprises:

a solid state device pluggable into a standard PC slot;

a non-accessible and non-visible circuit card embedded on said solid state device;

a connector for a network or similar communication medium; and

a circuitry able to detect the disconnection of said solid state device from the PC.

9. A method for secure communication encryption utilizing a combination of hardware and software comprising:

bundling of information into a message package;

sending information via a Transmitting Device;

receiving information via a Recipient Device; and

executing algorithms for encryption, decryption and registration of component devices.

10. A method as recited in claim 9 wherein said message package may precede or be appended to all messages and comprises:

a non-encrypted message Key; and

an identification of the sending device hardware.

11. A method as recited in claim 9 wherein said sending of information comprises:

registering said recipient device;

establishing a master key that is locally stored;

implementing software programs to prevent access to account keys;

executing an encryption algorithm;

allowing real time audio or audio/visual communications; and

sending files.

12. A method as recited in claim 9 wherein said receiving of information comprises:

receiving files;

allowing the real-time audio or audio/visual conversations over a digital network;

executing a decryption algorithm;

registering said transmitting device;

establishing a master Key that is locally stored; and

implementing software programs to prevent access to account Keys.

13. A method as recited in claim 12 wherein said receiving of information occurs with respect to communications between a Recipient Device and a plurality of Transmitting Devices.

14. A method as recited in claim 9 wherein the encryption, decryption and registration method comprises the steps of:

formatting a master Key from sub-key components;

incorporating into the Key generation, the date and message number;

retaining the master Key in memory;

matching the information of the device on the opposite end of the communication with the information contained within the Key;

allowing registration at any time of the day or night within a short time frame (a period of less than 30 seconds); and

separating the Key from the data transmission.

15. The method as recited in claim 14 wherein said master Key is formatted from sub-key components that include:

user account Key;

recipient account Key;

Sending Device authentication Key;

Recipient Device authentication Key;

Date and message number; and

certificate of authenticity.

16. A method as recited in claim 14 wherein said formatting of master Key comprises the steps of:

Generating new User Account Numbers (UAN) in the Recipient Device;

accepting a manually entered User Account Number (UAN) in the sending device;

creating a User Account Key (UAK) associated with the user account number (UAN);

connecting the Sending Device with the Recipient Device and transmitting the UAN;

verifying the received UAN and responding with a recipient account Key (RAK);

sending a UAK in response to an RAK; and

performing an exclusive or of RAK and UAK on both ends for the communication to obtain a master authentication Key.